PTO/SB/08A	(Substitut	e for form 1449/PTO)	· · · · · · · · · · · · · · · · · · ·		Atto	rney Docket I	No.: 004-9388		
	,		<del>,</del>	<del></del>		ication No.:	10/626,420		
IN	FORMAT	TION DISCLOSURE STATE	MENT BY APPLIC	ANT			ntor: Sheueling Chang Sha	ıntz	
-, 3 8 11-		(Use several sheets if nec			_	g Date:	July 24, 2003		
	*,5				-	p Art Unit:	2/3/		
BE 1 B MUS	· .	<del></del>		-		niner Name:	Ayaz R. Sheikh		
1150	C				Date	Submitted:	December 7, 2004		
C READER!	-		U.S. PATENT DO	CUMENTS					
Examiner Initials*	Cite No.1					Name of Patentee or Applicant of Cited Document		Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	
CJ		US-5,121,431	06-09-1992	Wiener			•		
CJ		US-6,633,896 B1	10-14-2003	Moore et al.	pore et al.				
		US-							
		US-							
		US-							
		US-							
		US-				_			
		US-	•						
		US-							
		US-					· · · · · · · · · · · · · · · · · · ·		
		US-							
		US-							
		F	OREIGN PATENT	DOCUMENTS					
Examiner Initials*	Cite No.1	Foreign Patent Document Country Code <sup>3</sup> -Number <sup>4</sup> -Kind Code <sup>5</sup> (if known)	Publication Date MM-DD-YYY		ne of Patentee or Applicant of Cited Document		Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T <sup>6</sup>	
		EP 0 247 383 A3	12-02-1987	Hasebe					
Examiner Si	gnature	/Carlton Joh	nnson/	Date Consider	red	01/22	2/2007		

<sup>\*</sup>EXAMISER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Applicant's unique citation designation number (optional).

See Kindo Codes of USPTO Patent Documents at we unipto gov or MPEP 901.04.

Senter Office that issued the document, by the two-letter code (MIPO Standard ST.1).

Por Japanese patent documents, the indication of the year of the reign of the Emperor must precede the sorial number of the patent document.

Kind of document by the appropriate pymbols as indicated on the document under MIPO Standard ST.16 if possible.

Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is collection by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CPR 1.14.

PTO/SB/08B (Substitute for form 1449/PTO) Attorney Docket No.: 004-9388 Application No.: 10/626,420 INFORMATION DISCLOSURE STATEMENT BY APPLICANT First Named Inventor: Sheueling Chang Shantz (Use several sheets if necessary) Filing Date: July 24, 2003 Group Art Unit: 2131 5.55 T 5 2035 Examiner Name: Ayaz R. Sheikh Date Submitted: December 7, 2004 Selve Benz NON PATENT LITERATURE DOCUMENTS T2 Examiner Cite Include name of author (in CAPITAL LETTERS), title of article (when appropriate), title of the item Initial\* No.1 (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. CJ Yvonne Hitchcock, et al., "Implementing an efficient elliptic curve cryptosystem over GF(p) on a smart card," ANZIAM J. 44(E), April 2003, pp. C354-C377. CJ National Institute of Standards and Technology, "Recommended Elliptic Curves for Federal Government Use," August 1999, 43 pages. Hasegawa, Toshio, et al., "A Practical Implementation of Elliptic Curve Cryptosystems over GF(p) on a 16-bit CJ Microcomputer," In Public Key Cryptography PKC '98, vol. 1431 of Lecture Notes in Computer Science, pages 182-194. /Carlton Johnson/ **Date Considered Examiner Signature** 01/22/2007

<sup>\*</sup>BRANINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Applicant's unique citation designation number (optional).

Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14.

	(Including name of a volume-isst Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October , 2002, 2 pages.  Groβschädl, Johann, "Instruction Proceedings of the 14th Symposium Koç, Cetin Kaya, "High-Speed Resolution Standards for Efficient Cryptogram September 20, 2000, pp. 1-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	ENT BY APPLICANT sary)  ATENT LITERATURE DO Butther in capital letters, titl ue number(s), publisher, ci gh Performance On Security ecture Software Developer's Set Extension for Long Inter om on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome uphy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	le of article, title of item, date, p ity and/or country where publis Algorithms (RSA Decryption Ko s Manual, Volume 1: Application reger Modulo Arithmetic on RISC e and High Performance Computer on 2.0, RSA Laboratories, Novement Multiplication to the Great D ed Elliptic Curve Domain Parameted	Sheueling Chang Shantz et al.  July 24, 2003 3621  July 1, 2004  Pertinent pages, hed.)  Ernel)," Intel Corporation, architecture," Revision  Based Smart Cards," ting, 2002, 7 pages.  Inber, 1994, pp. i-70.  Evide," Sun Microsystems  Eters," Certicom Research, ards Without					
*Examiner Initial No.  CJ AA  CJ AB  CJ AC  CJ AC  CJ AA  CJ AA  CJ AF  CJ AF  CJ AF  CJ AA  CJ AJ	NON PA  (Including name of a volume-iss  Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October, 2002, 2 pages.  Groβschädl, Johann, "Instruction Proceedings of the 14th Symposiu Koç, Cetin Kaya, "High-Speed R  Shantz, Sheueling Chang, "From June 2001, pp. 1-10.  Standards for Efficient Cryptogra September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	Sary)  ATENT LITERATURE DO Butthor in capital letters, titl ue number(s), publisher, ci gh Performance On Security ecture Software Developer's Set Extension for Long Inter om on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome uphy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	Applicant(s):  Filing Date:  Group Art Unit:  Date Submitted:  DCUMENTS  de of article, title of item, date, point and/or country where publis algorithms (RSA Decryption Keess Manual, Volume 1: Application and High Performance Computer and High Performance Computer Multiplication to the Great Deed Elliptic Curve Domain Parameter Curve Cryptography on Smart Cerval Country	Sheueling Chang Shantz et al.  July 24, 2003  3621  July 1, 2004  Pertinent pages, thed.)  Pernel)," Intel Corporation, an Architecture," Revision  -Based Smart Cards," ting, 2002, 7 pages.  Pathology of the pages of the page of the p					
Examiner Initial No.  CJ AA  CJ AB  CJ AC  CJ AC  CJ AA  CJ AA  CJ AA  CJ AF  CJ AF  CJ AA  CJ AJ	NON PA  (Including name of a volume-iss  Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October, 2002, 2 pages.  Groβschädl, Johann, "Instruction Proceedings of the 14th Symposiu Koç, Cetin Kaya, "High-Speed R  Shantz, Sheueling Chang, "From June 2001, pp. 1-10.  Standards for Efficient Cryptogra September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	Sary)  ATENT LITERATURE DO Butthor in capital letters, titl ue number(s), publisher, ci gh Performance On Security ecture Software Developer's Set Extension for Long Inter om on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome uphy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	Filing Date:  Group Art Unit:  Date Submitted:  DCUMENTS  The of article, title of item, date, proceeding and/or country where published algorithms (RSA Decryption Konstant), Volume 1: Application and High Performance Computer and High Performance Computer Multiplication to the Great Deed Elliptic Curve Domain Parameter Curve Cryptography on Smart Courve Cryptog	et al.  July 24, 2003  3621  July 1, 2004  Pertinent pages, hed.)  ernel)," Intel Corporation, architecture," Revision  -Based Smart Cards," ting, 2002, 7 pages.  Inber, 1994, pp. i-70.  Evide," Sun Microsystems  eters," Certicom Research, ards Without					
Examiner Initial No.  CJ AA  CJ AB  CJ AC  CJ AD  CJ AE  CJ AF  CJ AF  CJ AF  CJ AH  CJ AI	NON PA  (Including name of a volume-issel Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October, 2002, 2 pages.  Groβschädl, Johann, "Instruction Proceedings of the 14th Symposium Koç, Cetin Kaya, "High-Speed Research Shantz, Sheueling Chang, "From June 2001, pp. 1-10.  Standards for Efficient Cryptogram September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	attent Literature Double of the number (s), publisher, city performance On Security ecture Software Developer's Set Extension for Long Integration on Computer Architecture SA Implementation," Version Euclid's GCD to Montgome 19th, "SEC 2: Recommende V., Paar, Christof, "Elliptic	Group Art Unit:  Date Submitted:  DCUMENTS  The of article, title of item, date, point and/or country where publis algorithms (RSA Decryption Kots Manual, Volume 1: Application and High Performance Computer and High Performance Computer Multiplication to the Great Deed Elliptic Curve Domain Parameter Curve Cryptography on Smart Courve Cryptography on Smart Courv	July 1, 2004  pertinent pages, hed.)  pernel)," Intel Corporation, an Architecture," Revision  -Based Smart Cards," ting, 2002, 7 pages.  pher, 1994, pp. i-70.  ivide," Sun Microsystems  eters," Certicom Research, ards Without					
Examiner Initial No.  CJ AA  CJ AB  CJ AC  CJ AD  CJ AE  CJ AF  CJ AF  CJ AF  CJ AH  CJ AI	(Including name of a volume-isst Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October , 2002, 2 pages.  Groβschädl, Johann, "Instruction Proceedings of the 14th Symposium Koç, Cetin Kaya, "High-Speed Resolution Standards for Efficient Cryptogram September 20, 2000, pp. 1-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	nuthor in capital letters, titl ue number(s), publisher, cigh Performance On Security ecture Software Developer's Set Extension for Long Integration on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome 19thy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	Date Submitted: DCUMENTS  The of article, title of item, date, puty and/or country where publish Algorithms (RSA Decryption Kots Manual, Volume 1: Application and High Performance Computer on 2.0, RSA Laboratories, Novement Multiplication to the Great Deed Elliptic Curve Domain Parameter Curve Cryptography on Smart Courve Cryptograph	July 1, 2004  pertinent pages, hed.)  pernel)," Intel Corporation, an Architecture," Revision  -Based Smart Cards," hing, 2002, 7 pages. hber, 1994, pp. i-70.  ivide," Sun Microsystems  eters," Certicom Research, hards Without					
*Examiner Initial No.  CJ AA  CJ AB  CJ AC  CJ AD  CJ AE  CJ AF  CJ AF  CJ AF  CJ AA  CJ AJ	(Including name of a volume-isst Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October , 2002, 2 pages.  Groβschädl, Johann, "Instruction Proceedings of the 14th Symposium Koç, Cetin Kaya, "High-Speed Resolution Standards for Efficient Cryptogram September 20, 2000, pp. 1-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	nuthor in capital letters, titl ue number(s), publisher, cigh Performance On Security ecture Software Developer's Set Extension for Long Integration on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome 19thy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	DCUMENTS  le of article, title of item, date, p ity and/or country where publis Algorithms (RSA Decryption Ke is Manual, Volume 1: Application in Eger Modulo Arithmetic on RISC is and High Performance Compute ion 2.0, RSA Laboratories, Noven iery Multiplication to the Great D ied Elliptic Curve Domain Parame Curve Cryptography on Smart Ci	pertinent pages, thed.)  ernel)," Intel Corporation, an Architecture," Revision  -Based Smart Cards," ting, 2002, 7 pages. anber, 1994, pp. i-70.  ivide," Sun Microsystems eters," Certicom Research, ards Without					
*Examiner Initial No.  CJ AA  CJ AB  CJ AC  CJ AD  CJ AE  CJ AF  CJ AF  CJ AF  CJ AA  CJ AJ	(Including name of a volume-isst Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October , 2002, 2 pages.  Groβschädl, Johann, "Instruction Proceedings of the 14th Symposium Koç, Cetin Kaya, "High-Speed Resolution Standards for Efficient Cryptogram September 20, 2000, pp. 1-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	nuthor in capital letters, titl ue number(s), publisher, cigh Performance On Security ecture Software Developer's Set Extension for Long Integration on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome 19thy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	le of article, title of item, date, p ity and/or country where publis Algorithms (RSA Decryption Ko s Manual, Volume 1: Application reger Modulo Arithmetic on RISC e and High Performance Computer on 2.0, RSA Laboratories, Novement Multiplication to the Great D ed Elliptic Curve Domain Parameted	ernel)," Intel Corporation, In Architecture," Revision Based Smart Cards," ting, 2002, 7 pages. Inber, 1994, pp. i-70. Ivide," Sun Microsystems eters," Certicom Research, ards Without					
Initial No.  CJ AA  CJ AB  CJ AC  CJ AD  CJ AE  CJ AF  CJ AF  CJ AI  CJ AI	volume-iss  Intel® Itanium™ Processor, "Hig 2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October, 2002, 2 pages.  Großschädl, Johann, "Instruction Proceedings of the 14th Symposium Koç, Cetin Kaya, "High-Speed Research Shantz, Sheueling Chang, "From June 2001, pp. 1-10.  Standards for Efficient Cryptogra September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	the number(s), publisher, city Performance On Security ecture Software Developer's Set Extension for Long Integration on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome 19thy, "SEC 2: Recommended V., Paar, Christof, "Elliptic	Algorithms (RSA Decryption Kos Manual, Volume 1: Application and High Performance Computer and High Performance Computer Multiplication to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Computer Computer Computer Computer Computer Multiplication to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Computer Comp	ernel)," Intel Corporation, In Architecture," Revision Based Smart Cards," ting, 2002, 7 pages. Inber, 1994, pp. i-70. Ivide," Sun Microsystems eters," Certicom Research, ards Without					
CJ AB  CJ AC  CJ AD  CJ AE  CJ AF  CJ AF  CJ AG  CJ AH  CJ AI	2001, pp. 1-8.  Intel®, "Intel® Itanium™ Archit 2.1, October, 2002, 2 pages.  Großschädl, Johann, "Instruction Proceedings of the 14th Symposiu Koç, Cetin Kaya, "High-Speed R.  Shantz, Sheueling Chang, "From June 2001, pp. 1-10.  Standards for Efficient Cryptogra September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	Set Extension for Long Interm on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome The phy, "SEC 2: Recommended Section 1988 (1988)	eger Modulo Arithmetic on RISC e and High Performance Compute on 2.0, RSA Laboratories, Novemery Multiplication to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Circums 12 Application to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Domain Parameter Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application to the Great Ded Elliptic Curve Cryptography on Smart Circums 2 Application 2 Applicati	-Based Smart Cards," ting, 2002, 7 pages. hber, 1994, pp. i-70. ivide," Sun Microsystems eters," Certicom Research,					
CJ AC  CJ AD  CJ AE  CJ AF  CJ AF  CJ AH  CJ AI  CJ AJ	<ul> <li>2.1, October, 2002, 2 pages.</li> <li>Großschädl, Johann, "Instruction Proceedings of the 14<sup>th</sup> Symposiu Koç, Cetin Kaya, "High-Speed R</li> <li>Shantz, Sheueling Chang, "From June 2001, pp. 1-10.</li> <li>Standards for Efficient Cryptogra September 20, 2000, pp. i-45.</li> <li>Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.</li> <li>H. Cohen, A. Miyaji, and T. Ono</li> </ul>	Set Extension for Long Integration on Computer Architectur SA Implementation," Version Euclid's GCD to Montgome The phy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	eger Modulo Arithmetic on RISC e and High Performance Comput on 2.0, RSA Laboratories, Noven ery Multiplication to the Great D ed Elliptic Curve Domain Parame Curve Cryptography on Smart C	-Based Smart Cards," ting, 2002, 7 pages. nber, 1994, pp. i-70. ivide," Sun Microsystems eters," Certicom Research,					
CJ AD  CJ AE  CJ AF  CJ AG  CJ AH  CJ AI  CJ AJ	Proceedings of the 14th Symposium Koç, Cetin Kaya, "High-Speed Rown, Shantz, Sheueling Chang, "From June 2001, pp. 1-10.  Standards for Efficient Cryptogras September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	SA Implementation," Version Euclid's GCD to Montgomer Imphy, "SEC 2: Recommended V., Paar, Christof, "Elliptic	e and High Performance Computer 2.0, RSA Laboratories, Novemery Multiplication to the Great Dead Elliptic Curve Domain Parameter Curve Cryptography on Smart Computer 2.	ting, 2002, 7 pages.  Ther, 1994, pp. i-70.  Therefore, "Sun Microsystems  Eters," Certicom Research,  Tards Without					
CJ AE  CJ AF  CJ AH  CJ AI  CJ AJ	Shantz, Sheueling Chang, "From June 2001, pp. 1-10.  Standards for Efficient Cryptogra September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	Euclid's GCD to Montgome	ery Multiplication to the Great D ed Elliptic Curve Domain Parame Curve Cryptography on Smart C	ivide," Sun Microsystems eters," Certicom Research, ards Without					
CJ AF  CJ AH  CJ AI  CJ AJ	June 2001, pp. 1-10.  Standards for Efficient Cryptogras September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	uphy, "SEC 2: Recommende V., Paar, Christof, "Elliptic	ed Elliptic Curve Domain Parame	eters," Certicom Research, ards Without					
CJ AH  CJ AI  CJ AJ	September 20, 2000, pp. i-45.  Woodbury, A.D.; Bailey, Daniel Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono	V., Paar, Christof, "Elliptic	Curve Cryptography on Smart C	ards Without					
CJ AH  CJ AI  CJ AJ	Coprocessors," The Fourth Smart pp. 71-92.  H. Cohen, A. Miyaji, and T. Ono								
CJ AJ									
CJ AJ	H. Cohen, A. Miyaji, and T. Ono, "Efficient elliptic curve exponentiation using mixed coordinates", in K. Ohta and D. Pei, editors, Advances in Cryptology ASIACRYPT 98, pp. 51-65, Springer Verlag, 1998, LNCS 1514								
A.V.	D. Bailey and C. Paar, "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms." In H. Krawczyk, editor, Advances in Cryptography – CRYPTO '98, volume LNCS 1462, pages 472-485. Springer-Verlag, 1998. <a href="http://citeseer.ist.psu.edu/article/bailey98optimal.html">http://citeseer.ist.psu.edu/article/bailey98optimal.html</a> , 14 pages.								
C.T. AK	H. Pietiläinen, "Elliptic Curve Cryptography on Smart Cards," Master's Thesis, Helsinki University of Technology, Oct. 12, 2000, pp. i-81.								
CU	F. Morain and J. Olivos, "Speeding Up the Computations on an Elliptic Curve Using Addition-Subtraction Chains," Rapport de Recherche 983, INRIA, France, March 1989, <a href="http://citeseer.ist.psu.edu/morain90speeding.html">http://citeseer.ist.psu.edu/morain90speeding.html</a> , pp. 119-130.								
AL	,								
АМ									
AN									
AO									
AP				<del>.</del>					
AQ	· · · · · · · · · · · · · · · · · · ·								
Examiner /Carlt	on Johnson/ Date Cons	o2/24/200	7						